REMARKS

I. Claims 1-40 were rejected under 35 U.S.C. 102(e) as being anticipated by Cam Winget et al (Cam Winget), U.S. Patent Pub. No. 200510141498. Further, the office action provided that Cam Winget provides in paragraph 19, "said management frames being protection capable or non-protection capable and wherein said management frames indicate whether or not they are protection capable (0019)".

Applicant respectfully submits that paragraph 19 of Cam Winget provides:

> [0019] Throughout this description, the preferred embodiment and examples shown should be considered as exemplars, rather than limitations, of the present invention. The present invention provides a detection-based defense to a wireless network. Elements of the infrastructure, e.g., access points or scanning-only access points or other components (e.g., Infrastructure nodes) on the network, detect intruders by detecting spoofed frames, such as from rogue access points. Access points and other elements of the infrastructure include a signature, such as a management frame protection information element (MFP IE), with their management frames in a manner that enables neighboring access points or other network components to be able to validate the management frames, and to detect spoofed frames.

Given the language in Paragraph 19 and throughout the description of Winget, it is clear that the cited art does not provided "said Management Frames being protection-capable or non-protection-capable and wherein said Management Frames indicate whether or not they are protection-capable" as provided in the independent claims of the present invention. The MFP IE of Winget provides the validation of management frames and to detect spoofed frames. In contrast the present invention is designed to provide an indication of management frames that are capable of being protected and those that are not. This functionality is vital to make the present

invention backward compatible. Thus, devices that are not capable of protecting management frames can still be used with the present invention. Winget merely provides that all management frames are protected by the MFP IE and thus would not be backward compatible – a key element of the claimed invention.

This functionality and the importance of the two classes of frames is set forth in the present application as follows:

> One embodiment of the present invention provides a mechanism to protect Management Frames, such as Action Frames, and enables Wireless Stations (STAs) to exchange Management Frames, such as Action Frames, in a secure manner. In this preferred embodiment of the present invention a new attribute of the Action Frame is created and depends on whether or not the Action Frame can be protected. This result is two classes of Action Frames: protection-capable frames and non-protection-capable Frames. By default, all Action Frame are non-protection-capable, for backward compatibility. Non-protection-capable Actions Frames will be "normal" Action Frames – protection never applied. protection-capable Action Frames can be protected and will be protected if local policy requires. For example, if the Basic Service Set (BSS) policy does not require protected Action Frames, then STAs shall send all Action Frames without protection, including all protection-capable Action Frames.

As the type of protection is not the focus of the invention, unlike Winget, the present invention provides numerous types of management frame protection as follows:

> Once STAs negotiation is finished, the protection-capable Action Frame is protected in the same ways as an ordinary data MPDU if local policy requires the protection-capable Action Frame to be protected. FIG. 4, shown generally as 400, illustrates the TKIP MPDU Format, with header part 405 and data frames 410. An expanded view of data frames 410 is shown by reference numerals 415 – 435, with IV/KeyID (4 octets) 415, Extended IV (4 octets) 420, Data (>= 1 octets) 425, MC (8 octets) 430 and ICV (4 octets) 435. The encrypted portion 412, includes Data 425, MC

430 and ICV435. An expanded view of IV/Key ID 415 is illustrated at 440 and 445; and an expanded view of Extended IV is illustrated at 450.

Another method of protection is accomplished by applying the IEEE 802.11i CCMP protocol construction to protection-capable Action Frames. FIG. 5, shown generally as 500, illustrates the CCMP MPDU Format of one preferred embodiment of the present invention. Header part is illustrated at 505 and data portion at 510. The data portion 510 is expanded to show IV/Key ID (4 octets) 515, Extended IV (4 octets) 520, Data (Octets >= 0) 525, and MIC (8 octets) 530. IV/Key ID 515 is shown expanded at 535 and Extended IV is expanded at 540.

The CCMP Message Integrity Code protects the Action Frame from undetected forgery. The CCMP Sequence Number protects the Action Frame from replay. The CCMP encryption scheme maintains the Action Frame payload as confidential. Sender's Pairwise Temporal Key protects unicast Action Frame and Sender's Group Temporal Key is used to protect broadcast/multicast Action Frame. An important benefit of the present invention allows the same keys that are used for data and thus no additional key management scheme required.

Based on the reasons set forth above, Applicant respectfully submits that the rejection of claims 1-40 under 35 U.S.C. 102(e) as being anticipated by Cam Winget et al (Cam Winget), U.S. Patent Pub. No. 200510141498 has been traversed.

CONCLUSION

In light of at least the foregoing amendments and remarks, Applicant respectfully submits that claim 1 – 40 are in condition for allowance and such action is earnestly solicited. ***The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.***

Please charge any shortages and credit any overcharges to our Deposit Account number 50-0221.

Respectfully submitted,

Date: October 29, 2007

by:/s/James S. Finn/Reg. No., 38,450/
James S. Finn
Reg. No. 38,450
Attorney for Assignee Intel Corporation

Intel Corporation
c/o Intellevate, LLC
P.O. Box 52050
Minneapolis, MN 55402
202-607-4607